(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 February 2002 (21.02.2002)

PCT

(10) International Publication Number
WO 02/15579 A1

(51) International Patent Classification⁷: H04N 7/167, 7/173

(21) International Application Number: PCT/US00/11891

(22) International Filing Date: 2 May 2000 (02.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tournament Drive, Horsham, PA 19044 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: SO, Nicol, Chung, Pang [CN/US]; 1829 Finch Drive, Bensalem, PA 19020 (US).

(74) Agent: LIPSITZ, Barry, R.; 755 Main Street, Building No. 8, Monroe, CT 06468 (US).

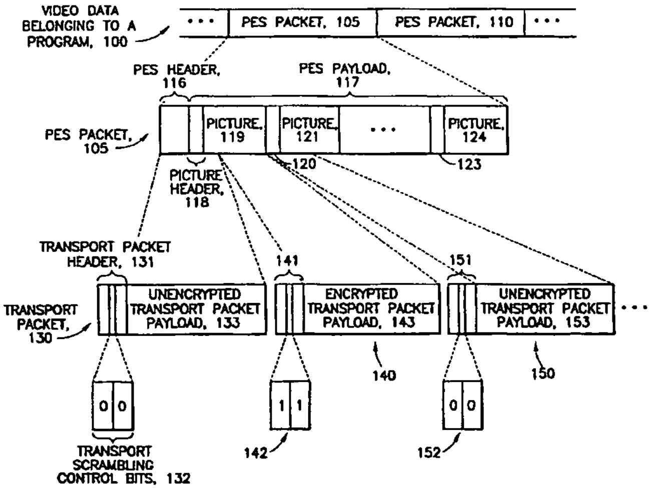
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR ENABLING RANDOM ACCESS TO INDIVIDUAL PICTURES IN AN ENCRYPTED VIDEO STREAM


VIDEO DATA BELONGING TO A PROGRAM, 100
PES PACKET, 105
PES PACKET, 110
PES HEADER, 116
PES PAYLOAD, 117
PES PACKET, 105
PICTURE, 119
PICTURE, 121
PICTURE, 124
120
123
PICTURE HEADER, 118
TRANSPORT PACKET HEADER, 131
141
151
TRANSPORT PACKET, 130
UNENCRYPTED TRANSPORT PACKET PAYLOAD, 133
ENCRYPTED TRANSPORT PACKET PAYLOAD, 143
UNENCRYPTED TRANSPORT PACKET PAYLOAD, 153
140
150
0 0
1 1
0 0
TRANSPORT SCRAMBLING CONTROL BITS, 132
142
152

(57) Abstract: A system for providing conditional access to packetized picture (video), audio or other data. The system selectively encrypts packetized data (105) such that transport packets (130, 150) that include header data (131, 151) are unencrypted, while all other transport packets (140, 141) that do not include header data are encrypted. This allows the transport packets with the header data (130, 150) to be randomly accessed from a memory (230, 310), which is particularly advantageous for performing "trick modes", such as fast forward and fast reverse, e.g., in a video-on-demand service. After the transport packets are selectively encrypted and stored, transport scrambling and control bits (132, 142, 152) for each packet (130, 140, 150) can be accessed to determine whether the packet is encrypted, and consequently, whether the packet includes header data. If a packet includes header data, it is suitable for use in a trick mode since it provides data from the start of a video, audio or other data packet.

WO 02/15579 A1

METHOD AND APPARATUS FOR ENABLING RANDOM ACCESS TO INDIVIDUAL PICTURES IN AN ENCRYPTED VIDEO STREAM

BACKGROUND OF THE INVENTION

The present invention relates to an encrypted packetized data processing system. The invention is particularly suited for use in a video-on-demand (VOD) system wherein motion control ("trick modes"), such as fast forward and fast reverse modes, are required.

Video-on-demand (VOD) is an interactive video service typically provided over a point-to-multipoint distribution system, such as a cable television system. With VOD, a subscriber can order video (such as a movie, sport event or the like) or other types of content at any time, without adhering to a pre-defined showing schedule. A full-function VOD system provides the subscriber with Video Cassette Recorder (VCR)-like motion control functions, such as pause (freeze frame), fast forward, fast reverse, and slow reverse. These functions, variously known as trick play, trick mode, or motion control, enhance the subscriber's viewing experience and mimic (or exceed) the level of control subscribers expect from conventional video tapes, such as those which can be commonly purchased or rented.

In a VOD system, content is stored in video servers, which are specialized high-capacity file servers. The content is played from stored files upon purchase by a subscriber. To facilitate remultiplexing and error correction, digital video content is typically packetized into fixed-size units. Such is that case in the popular MPEG-2 standard (ITU-T Rec. H.222.0 ISO/IEC 13818) used in digital television.

To perform motion control, a video server controller responds to motion control commands from set-top boxes and changes the way content is played back. In fast forward and fast reverse, the video server will skip selected pictures to create a sped-up version of the video. Depending on the method employed, it may be necessary to have fast, random access to the individual pictures in a video file. To reduce storage requirements and to allow flexible control of the speed-up factor, pictures in fast forward and fast reverse sequences are often extracted in real time from the normal video file, which contains all pictures in the movie or other program.

There are two ways to search for pictures to be displayed in a scan forward/backward sequence. The first is to scan the main video file sequentially looking for starts of pictures. The other method is to build an auxiliary index file to the start points of pictures in the main video file.

However, another concern is controlling access to the VOD programming, e.g., to maintain the financial viability of the system. Specifically, a conditional access scheme is implemented to deny access to services or content by unauthorized parties. Conditional access requires a trustworthy mechanism for classifying users into different groups, and an enforcement mechanism for denying access to groups of unauthorized users.

Encryption is often used to control access to the content carried by carrier signals. The conventional approach to encrypting content for VOD distribution is to have real-time encrypting devices on the delivery path between the video server and the subscribers. This approach works well when the number of subscribers is relatively small. However, as the number of subscribers increases, the number of encrypting devices and their physical space requirements become burdensome. This space problem does not exist with traditional broadcast type services because the same content stream is shared by all subscribers and the number of encrypting devices does not increase with the number of subscribers.

An alternative to real-time encryption of VOD content is off-line, pre-encryption. In this approach, video content is processed and encrypted before it is loaded into video servers. The advantage of pre-encryption is that it removes the need for encrypting devices on the video delivery path, thus making VOD service substantially less expensive and more scalable. The pre-encryption can be done centrally at a content preparation site, which is separate from the locations (headends) at which the VOD service is deployed. Once video is pre-encrypted at the central site, the same encrypted copies can be distributed to multiple headends where VOD is deployed.

However, pre-encrypting VOD content creates a problem: it interferes with the detection of the location of the starting point of individual pictures in a video file. In general, video servers do not have the capability or authorization to decrypt pre-encrypted video content. As a result, they cannot locate individual pictures in an encrypted video file just by scanning the file. A similar problem is confronted when the encrypted content is stored at a decoder prior to display, where it is time consuming and computationally intensive to have to decrypt all of the pictures to locate specific pictures.

Accordingly, it would be desirable to provide a system that addresses the above problems.

The system should enable random access to individual pictures in an encrypted video file for use in modes such as fast forward, fast reverse, pause, resume, slow motion (forward or reverse), frame-by-frame or other incremental frame advance or scan (e.g., advancing N frames at a time, where N>1), and the like.

The system should allow a secure video-on-demand system to be deployed at a reduced cost.

The system should be compatible with packetized data communication schemes, such as MPEG-2.

The invention should be compatible with a user device that stores an encrypted video file, such as a personal video recorder (PVR), personal computer hard disk or the like.

The present invention provides a system having the above and other advantages.

SUMMARY OF THE INVENTION

The present invention relates to an encrypted packetized data processing system.

In accordance with one aspect of the invention, a particular method for providing at least partially encrypted packetized data includes the step of receiving input digital data from a data source, such as a video server. The input digital data includes a plurality of encoded data segments with respective data headers, such as found in an MPEG-compatible Packetized Elementary Stream (PES) packet. The input digital data is subdivided for transport in successive transport packets such that at least two types of transport packets are provided, including a first type that includes at least a portion of an associated data header, and a second type that includes at least a portion of an associated encoded data segment but does not include any portion of the data headers.

The second type of transport packets are encrypted, while leaving the first type of transport packets unencrypted. Identifiers are provided for the respective transport packets to indicate whether the respective transport packet is encrypted or unencrypted.

This allows the transport packets with the header data to be randomly accessed from a memory, which is particularly advantageous for performing "trick modes", such as fast forward and fast reverse, e.g., in a video-on-demand service. If a packet includes header data, it is suitable for use in a trick mode since it provides data from the start of a video, audio or other data packet.

In a further aspect of the invention, a method for decoding at least partially encrypted packetized data includes the step of receiving successive transport packets from a transport stream. The transport packets are formed by subdividing digital data that includes a plurality of encoded data segments with respective data headers into a first, encrypted type that includes at least a portion of an associated data header, and a second, unencrypted type that includes at least a portion of an associated encoded data segment but does not include any portion of the data headers. Identifiers are provided for the respective transport packets to indicate whether the respective transport packet is encrypted or unencrypted.

The transport packets are stored in a storage device, and the identifiers are used to randomly access the first type of transport packets from the storage device without performing decryption. For example, a personal video recorder or other user device that stores the partially encrypted transport packets may be used. The packets are subsequently decrypted when the user desires to view the data.

Corresponding apparatuses are also presented.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates the formation of transport packets in accordance with the present invention.

FIG. 2 illustrates an encoder in accordance with the present invention.

FIG. 3 illustrates a user device/decoder in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention relates to an encrypted packetized data processing system.

FIG. 1 illustrates the formation of transport packets in accordance with the present invention.

To facilitate discussion, an implementation of the invention in a typical packetized digital video format, such as MPEG-2, is discussed. However, the present invention is applicable to other digital formats sharing similar features.

In the MPEG-2 format, video information is digitized and compressed before being encoded. The compression can be considered part of the encoding. Compressed video from a program 100 is divided into variable-length units called Packetized Elementary Stream (PES) packets, such as PES packets 105 and 110, each of which contains a variable number of encoded pictures. For example, the PES packet 105 includes encoded pictures 119, 121, . . . , 124.

The example PES packet 105 has a header 116 and a payload portion 117. Moreover, each picture in the PES packet 105 is prefixed by a header containing information about the picture. For example, the picture 119 has a header 118, the picture 121 has a header 120, and the picture 124 has a header 123.

For transmission and storage purposes, PES packets are further broken down into fixed-length units called transport packets, such as transport packets 130, 140 and 150. With the MPEG-2 standard, each transport packets comprises 188 bytes. Generally, the PES packet length is much larger than the size of a transport stream packet. Each transport packet has a header and a payload portion. The header of a transport packet contains, among other information, two transport scrambling control bits, which indicates the encryption (scrambling) status of the packet.

In the MPEG-2 standard, the scrambling control bits are designated by the field "transport_scrambling_control". A scrambling control value of "00" indicate the transport packet is not scrambled, while the values "01", "10", and "11" can be user-defined. The value "11" is used herein as an example to designate a scrambled or encrypted transport packet. Any type of analogous scheme may be used to indicate the encryption status of a transport packet.

The transport packet 130 includes a header 131, scrambling control bits 132 (which indicate an unencrypted transport packet), and a payload 133. The transport packet 140 includes a header 141, scrambling control bits 142 (which indicate an encrypted transport packet), and a payload 143. The transport packet 150 includes a header 151, scrambling control bits 152 (which indicate an unencrypted transport packet), and a payload 153.

Each transport packet is formed by subdividing the contents of successive portions of a PES packet. For example, the payload 133 of the transport packet 130 comprises the PES header 116, picture header 118, and a portion of the picture data 119 of the PES payload 117. The payload 143 of the transport packet 140 comprises a successive portion of the picture data 119 of the PES payload 117. The payload 153 of the transport packet 150 comprises the picture header 120, and a portion of the picture data 121 of the PES payload 117, and so on.

Note that FIG. 1 is shown in simplified form since, in practice, the data from one picture is usually carried in the payloads of several transport packets. Moreover, the amount of picture data (e.g., fields 119, 121, 124) is often much larger than the amount of the corresponding picture header data (e.g., fields 118, 120, 123, respectively). As a result, the majority of the transport packets will carry only picture data but no picture header data, thereby resulting in most transport packets being encrypted, with relatively few transport packets being unencrypted. Thus, an unauthorized user who tunes to the mostly-encrypted program will not be able to watch the program with appreciable understanding.

The transport packets are assembled into a transport stream and transmitted to a user terminal (e.g., set-top box) typically via a satellite, cable or hybrid fiber/cable network, although communication via essentially any network, such as a computer network is also possible. If prepared at a central content preparation site, the transport stream may be provided to one or more headends before being provided to the user terminal.

Generally, the data can be prepared at a central preparation site, such as by a national supplier, at a headend, or each content vendor can arrange for its own content preparation, e.g., according to any special needs of its equipment.

As is known, a transport stream is a multiplex formed by interleaving transport packets belonging to one or more programs. Transport packets belonging to different programs in a transport stream are differentiated by a Packet Identifier (PID) in their headers. A single Program Transport Stream includes of transport packets of one program only.

FIG. 2 illustrates an encoder in accordance with the present invention. The encoder 200 comprises equipment for performing selective packet encryption. The depicted equipment may be located at a central content preparation site or at a headend, for example.

The present invention overcomes the problem of locating picture start points caused by the use of pre-encryption. This is achieved, as discussed, by leaving selected (transport stream) packets unencrypted in a video file. The equipment set-up 200 to achieve this includes one or more digital video sources 210, a pre-processing workstation 215 for generating auxiliary data files and for labeling selected packets for encryption, an encryption device 220, an encryption device controller 205, an optional post-processing workstation 225 for processing encrypted video (e.g., to adjust timing information that may be perturbed by the encryption process), and a storage device 230 for storing the processed data prior to providing it to a headend or end user.

In the encoder set-up 200, the digital video source 210 supplies the digital video stream to be encrypted. The video source may be a digital video encoder, or a file server playing back pre-encoded video files. The digital video stream is fed into the pre-processing workstation 215, whose main function is to identify and label transport packets for encryption. A packet is selected for encryption if it contains no picture header or portion thereof, and therefore need not be examined by the video server during motion control (trick modes). Transport packets selected for encryption are labeled by having the transport scrambling control bits set to some special value (e.g., "11").

Packets to be left unencrypted are similarly labeled, using a different special value (e.g. "00"). The pre-processing step may optionally generate auxiliary data files used in the delivery of VOD services.

Encryption of the pre-processed video stream is performed by the encryption device 220 under the control of the device controller 205, which is, in turn, responsive to encryption control parameters. Any suitable encryption scheme may be used. The encryption control parameters may include, e.g., information related to the program being encrypted, or the particular encryption session, or both. When encryption is performed, the encryption device 220 examines the transport scrambling control bits of each transport packet. Packets with those two bits set to, e.g., "00" are left unencrypted, while packets with the bits set to, e.g., "11" are encrypted.

The output of the encryption device 220, which comprises a selectively-encrypted video stream, is optionally put through a post-processing stage (e.g., workstation 225) before being stored in the storage device 230. Post-processing may or may not be needed depending on the design and implementation of the VOD service equipment.

To search for the starting point of pictures in a pre-encrypted video file during trick mode play, a video server scans the transport packets in a video file sequentially. The transport scrambling control bits in each transport packet headers indicate whether the packet is encrypted. If a packet is encrypted, it can be inferred that it contains no picture header. If a packet is unencrypted, the payload can be examined to locate the picture header.

A video server can still read other kinds of information embedded in a pre-encrypted video file, such as private data in an adaptation field of a transport packet header.

FIG. 3 illustrates a user device/decoder in accordance with the present invention.

Optionally, the program content can be temporarily stored at a user device/decoder prior to playing. The device may be a personal video recorder or other terminal or appliance in a user's home, or even a portable unit carried by the user or used in an automobile.

For example, rather than playing at a specified time under the control of a headend, a storage device containing the programming may be purchased or rented for subsequent re-play by the user. Under a purchase scenario, the user may enjoy unlimited replays, while under a rental scenario, a fixed number of replays or an expiration date may be enforced.

Or, the user may be given the option of storing the transport stream prior to playing.

Thus, the user device/decoder 300 can be provided with the capability for providing motion control (e.g., trick modes).

The decoder 300 may include a demultiplexer (demux)

302 that receives a transport stream with the encrypted and unencrypted transport packets, such as those previously stored at the storage device 230 in FIG. 2, and optionally other programming services. Other necessary components, e.g., for demodulation, error correction, synchronization and the like are not shown, but should be apparent to those skilled in the art.

The demux 302 extracts the encrypted and unencrypted packets that belong to a particular program. The extracted stream of packets either is stored in the memory 310, or is provided to a second demux 305, which separates the encrypted transport packets from the unencrypted transport packets. For example, an entire movie or the like may be stored in the memory 310 for subsequent retrieval and motion control. The memory 310 is analogous to the storage device 230 of FIG. 2.

The demux 305 includes a scrambling control bit identifier/detector 306 that identifies the scrambling control bits of each transport packet to determine if the packet is encrypted or unencrypted.

A control 335, such as a central processing unit (CPU), provide oversight of the various functions in the decoder 300.

A user interface 340 receives commands from a user, e.g., via a hand-held remote control, to view the content in a regular play mode or in a trick mode. In response to this request, the interface 340 provides a corresponding signal to the control 335, which commands the memory 310 to output the packets to the demux 305. A video/audio/data processing function 320 receives unencrypted packets from the decryptor 315 and demux 305.

The data from the function 320 is provided to an output device 325, such as a television, personal computer, speakers, and so forth. The output device 325 may provide a graphical user interface (GUI) or other mechanism to assist the user in playing the programming content in a normal or trick mode. The user may also place an order for the content via such an interface.

An optional upstream transmitter 330 transmits a user request, such as an order for VOD programming, to a headend or other network control facility. The user request may travel over the same or different channel from which the transport stream was received.

It should now be appreciated that the present invention provides a system for providing conditional access to packetized picture, audio or other data. The system selectively encrypts packetized data such that transport packets that include header data are unencrypted, while all other transport packets that do not include header data are encrypted. This allows the transport packets with the header data to be randomly accessed from a memory, which is particularly advantageous for performing trick modes, such as fast forward and fast reverse, e.g., in a video on demand service.

In particular, after the transport packets are selectively encrypted and stored, transport scrambling and control bits for each packet can be accessed to determine whether the packet is encrypted, and consequently, whether the packet includes header data. If a packet includes header data, it is suitable for use in a trick mode since it provides data from the start of a video, audio or other data packet.

Although the invention has been described in connection with various specific embodiments, those skilled in the art will appreciate that numerous adaptations and modifications may be made thereto without departing from the spirit and scope of the invention as set forth in the claims.

For example, the selectively encrypted transport packets need not be transmitted to a subscriber terminal, but may be provided in a storage device for subsequent retrieval by a user, such as in a personal video recorder (PVR).

What is claimed is:

1. A method for providing at least partially encrypted packetized data, comprising the steps of:

(a) receiving input digital data from a data source;

wherein the input digital data includes a plurality of encoded data segments with respective data headers;

(b) subdividing the input digital data for transport in successive transport packets such that at least two types of transport packets are provided, including a first type that includes at least a portion of the associated data header, and a second type that includes at least a portion of an associated encoded data segment but does not include any portion of the data headers;

(c) encrypting the second type of transport packets while leaving the first type of transport packets unencrypted; and

(d) providing identifiers for the respective transport packets to indicate whether the respective transport packet is encrypted or unencrypted.

2. The method of claim 1, wherein:

at least one of the second type of transport packets includes data from a plurality of the data segments.

3. The method of claim 1, wherein:

the input digital data is received in packetized elementary stream packets.

4. The method of claim 1, wherein:

the identifiers are provided in respective headers of the respective transport packets.

5. The method of claim 1, comprising the further step of:

storing the transport packets in a storage device;

wherein the identifiers enable the first type of transport packets to be randomly accessed from the storage device without performing decryption.

6. The method of claim 5, comprising the further step of:

randomly accessing at least one of the first type of transport packets to provide a trick mode for the transport packets.

7. The method of claim 6, wherein the trick mode comprises at least one of: fast forward, slow forward, fast reverse, slow reverse, pause, resume, and incremental frame motion.

8. The method of claim 5, wherein:

the storage device comprises a video server.

9. The method of claim 1, comprising the further steps of:

storing the transport packets in a storage device; and

in response to a user request, retrieving the transport packets from the storage device and providing the retrieved transport packets to a user device via a network.

10. The method of claim 9, wherein:
the retrieved transport packets are provided to the user device in a video-on-demand service.

11. The method of claim 9, comprising the further steps of:
providing information to the user for decrypting the second type of transport packets; and
providing a display from the first type of transport packets, and the decrypted second type of transport packets.

12. The method of claim 1, wherein:
the data source comprises a digital video encoder.

13. The method of claim 1, wherein:
the data source comprises a file server playing back pre-encoded video files.

14. The method of claim 1, wherein:
at least one of the first type of transport packets also includes at least a portion of an associated encoded data segment.

15. The method of claim 1, wherein:
the input digital data comprises at least one of video and audio data.

16. The method of claim 1, wherein:
the transport packets with the respective

identifiers are provided at a central content preparation site for subsequent distribution to at least one subscriber network headend.

17. A method for decoding at least partially encrypted packetized data, comprising the steps of:

(a) receiving successive transport packets from a transport stream; wherein:

the transport packets are formed by subdividing digital data that includes a plurality of encoded data segments with respective data headers into at least two types of transport packets, including a first type that includes at least a portion of an associated data header, and a second type that includes at least a portion of an associated encoded data segment but does not include any portion of the data headers;

the second type of transport packets are encrypted while the first type of transport packets are unencrypted; and

identifiers are provided for the respective transport packets to indicate whether the respective transport packet is encrypted or unencrypted;

(b) storing the transport packets in a storage device; and

(c) using the identifiers to randomly access at least one of the first type of transport packets from the storage device without performing decryption.

18. The method of claim 17, wherein:

at least some of the second type of transport packets include data from a plurality of the data segments.

19. The method of claim 17, wherein:

the digital data is subdivided from packetized elementary stream packets.

20. The method of claim 17, wherein said using step comprises the step of:

recovering the identifiers from the respective headers of the respective transport packets.

21. The method of claim 17, wherein:

at least one of the first type of transport packets is randomly accessed to provide a trick mode for the transport packets.

22. The method of claim 21, wherein the trick mode comprises at least one of: fast forward, slow forward, fast reverse, slow reverse, pause, resume, and incremental frame motion.

23. The method of claim 17, wherein:

the storage device comprises a decoder memory.

24. The method of claim 17, wherein:

the transport packets are provided to a user device in a video-on-demand service.

25. The method of claim 17, comprising the further steps of:

decrypting the second type of transport packets; and

providing a display from the first type of transport packets, and the decrypted second type of transport packets.

26. The method of claim 17, wherein:

at least one of the first type of transport packets also includes at least a portion of an associated encoded data segment.

27. The method of claim 17, wherein:

the digital data comprises at least one of video and audio data.

28. An apparatus for providing at least partially encrypted packetized data, comprising:

means for receiving input digital data from a data source;

wherein the input digital data includes a plurality of encoded data segments with respective data headers;

subdividing the input digital data for transport in successive transport packets such that at least two types of transport packets are provided, including a first type that includes at least a portion of the associated data header, and a second type that includes at least a portion of an associated encoded data segment but does not include any portion of the data headers;

means for encrypting the second type of transport packets while leaving the first type of transport packets unencrypted; and

means for providing identifiers for the respective transport packets to indicate whether the respective transport packet is encrypted or unencrypted.

29. An apparatus for decoding at least partially encrypted packetized data, comprising:

means for receiving successive transport packets from a transport stream; wherein:

the transport packets are formed by subdividing digital data that includes a plurality of encoded data segments with respective data headers into at least two types of transport packets, including a first type that includes at least a portion of an associated data header, and a second type that includes at least a portion of an associated encoded data segment but does not include any portion of the data headers;

the second type of transport packets are encrypted while the first type of transport packets are unencrypted; and

identifiers are provided for the respective transport packets to indicate whether the respective transport packet is encrypted or unencrypted;

means for storing the transport packets in a storage device; and

means for using the identifiers to randomly access at least one of the first type of transport packets from the storage device without performing decryption.

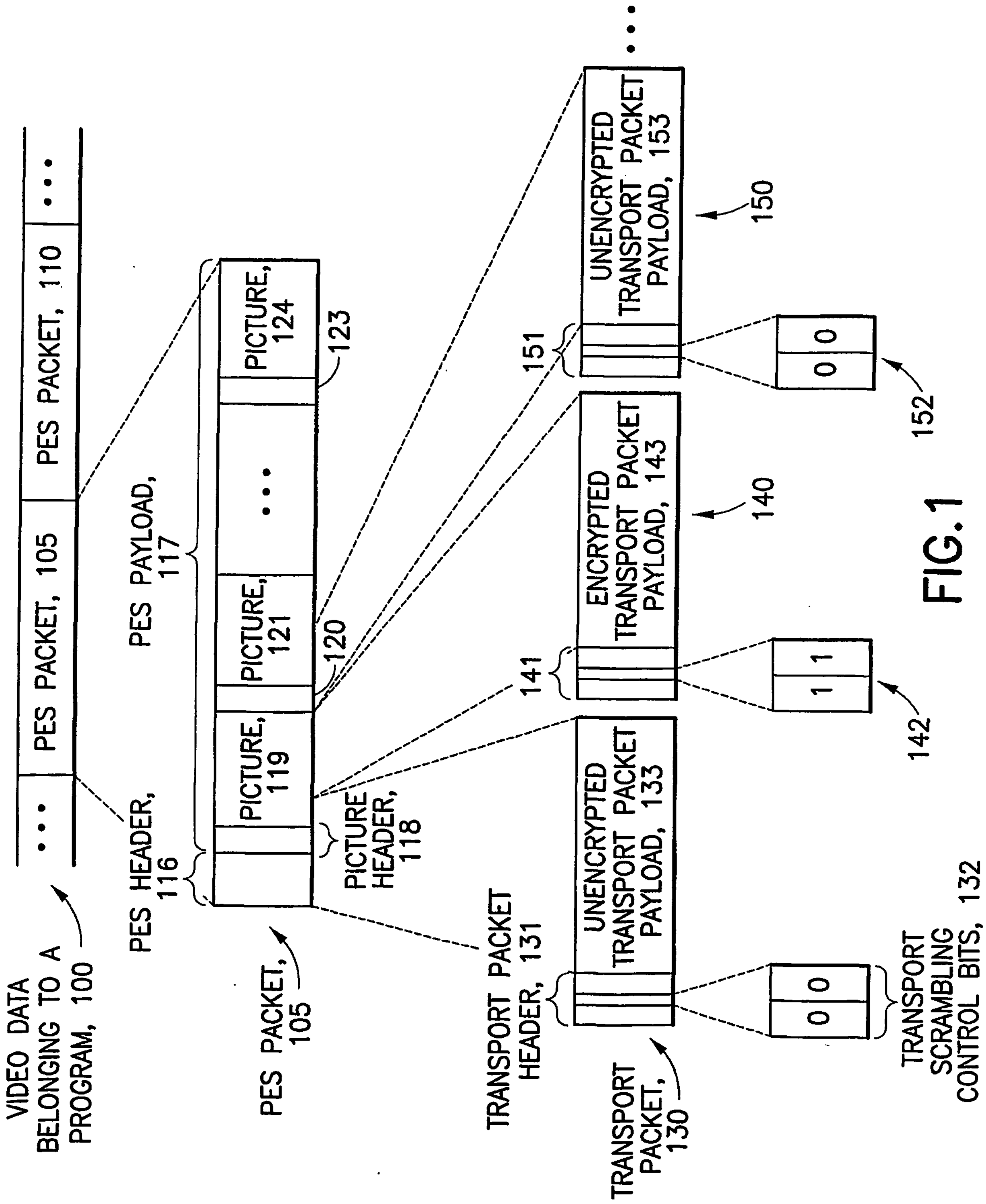

VIDEO DATA BELONGING TO A PROGRAM, 100
• • •
PES PACKET, 105
PES PACKET, 110
• • •
PES HEADER, 116
PES PAYLOAD, 117
PES PACKET, 105
PICTURE HEADER, 118
PICTURE, 119
120
PICTURE, 121
• • •
123
PICTURE, 124
TRANSPORT PACKET HEADER, 131
TRANSPORT PACKET, 130
UNENCRYPTED TRANSPORT PACKET PAYLOAD, 133
0 0
TRANSPORT SCRAMBLING CONTROL BITS, 132
141
ENCRYPTED TRANSPORT PACKET PAYLOAD, 143
1 1
142
140
151
UNENCRYPTED TRANSPORT PACKET PAYLOAD, 153
0 0
152
150
• • •

FIG.1

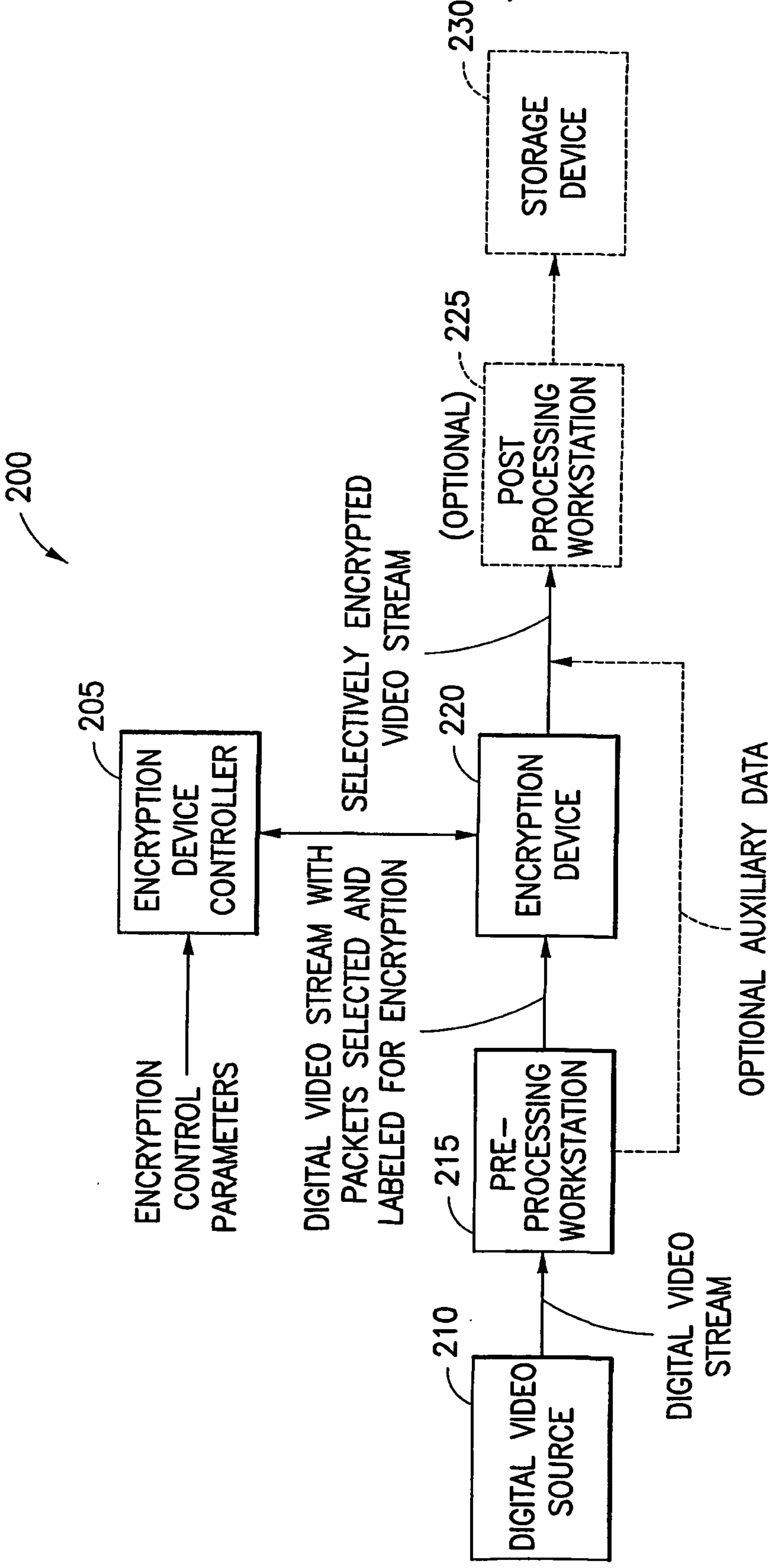

200
ENCRYPTION CONTROL PARAMETERS
205
ENCRYPTION DEVICE CONTROLLER
DIGITAL VIDEO STREAM WITH PACKETS SELECTED AND LABELED FOR ENCRYPTION
SELECTIVELY ENCRYPTED VIDEO STREAM
210
DIGITAL VIDEO SOURCE
DIGITAL VIDEO STREAM
215
PRE-PROCESSING WORKSTATION
220
ENCRYPTION DEVICE
(OPTIONAL)
225
POST PROCESSING WORKSTATION
230
STORAGE DEVICE
OPTIONAL AUXILIARY DATA

FIG.2

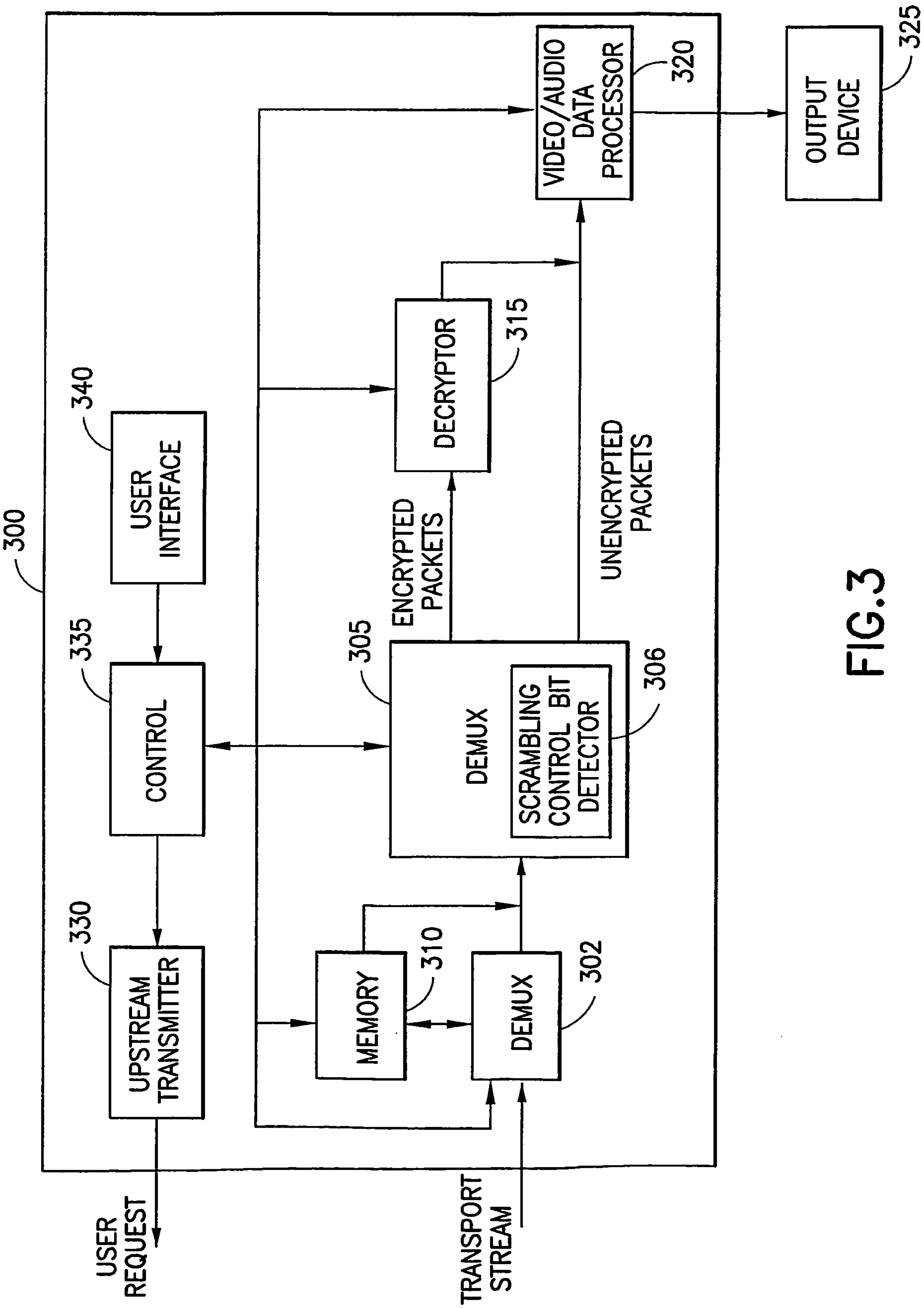

300
USER INTERFACE
340
CONTROL
335
UPSTREAM TRANSMITTER
330
USER REQUEST
TRANSPORT STREAM
DEMUX
302
MEMORY
310
DEMUX
305
SCRAMBLING CONTROL BIT DETECTOR
306
ENCRYPTED PACKETS
UNENCRYPTED PACKETS
DECRYPTOR
315
VIDEO/AUDIO DATA PROCESSOR
320
OUTPUT DEVICE
325

FIG.3

INTERNATI L SEARCH REPORT

Interr u ion No
PCT/US 00/11891

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04N7/173

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 714 204 A (LG ELECTRONICS INC) 29 May 1996 (1996-05-29) page 6, line 41 - line 42 page 3, line 20 - line 34 abstract ---	1,17,28, 29
A	EP 0 674 441 A (NOKIA TECHNOLOGY GMBH) 27 September 1995 (1995-09-27) column 6, line 50 -column 7, line 1 abstract ---	1,17,28, 29
A	WO 99 37072 A (APPLE COMPUTER) 22 July 1999 (1999-07-22) abstract page 22, line 11 - line 16 --- -/--	1,17,28, 29

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 12 December 2000	Date of mailing of the international search report 22/12/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Dockhorn, H

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/11891

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 964 578 A (ORACLE CORP) 15 December 1999 (1999-12-15) abstract -----	1,17,28, 29

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/11891

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
EP 714204	A	29-05-1996	CN	1137723	A	11-12-1996
			JP	8242438	A	17-09-1996
			US	5757909	A	26-05-1998
EP 674441	A	27-09-1995	FI	941315	A	22-09-1995
			DE	69506463	D	21-01-1999
			DE	69506463	T	10-06-1999
WO 9937072	A	22-07-1999	AU	2232799	A	02-08-1999
			AU	2232899	A	02-08-1999
			AU	2322499	A	02-08-1999
			EP	1051008	A	08-11-2000
			EP	1048156	A	02-11-2000
			WO	9937056	A	22-07-1999
			WO	9937057	A	22-07-1999
			US	6134243	A	17-10-2000
EP 0964578	A	15-12-1999	US	5659539	A	19-08-1997
			EP	0963117	A	08-12-1999
			EP	0963118	A	08-12-1999
			CA	2197323	A	06-02-1997
			EP	0781490	A	02-07-1997
			WO	9704596	A	06-02-1997
			US	5864682	A	26-01-1999
			US	6112226	A	29-08-2000
			US	6138147	A	24-10-2000
			US	6119154	A	12-09-2000